Глава 2. Аутентификация пользователей по протоколу PEAP-MSCHAPv2

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol — Microsoft Challenge Handshake Authentication Protocol version 2) — это протокол аутентификации в сети. Он сочетает использование протокола TLS для защиты канала и механизма проверки имени пользователя и пароля (MSCHAPv2) внутри этого зашифрованного соединения. Протокол описан в **RFC 4851** и широко применяется благодаря совместимости с инфраструктурой Active Directory и простоте настройки на клиентах.

В NAC-системах PEAP-MSCHAPv2 используется на этапе сетевой аутентификации. Когда пользователь подключается к сети, точка доступа или коммутатор (аутентификатор) перенаправляет его запрос на сервер аутентификации. Сервер предъявляет свой цифровой сертификат, клиент проверяет его подлинность и устанавливает защищенный TLS-туннель. Внутри этого туннеля происходит передача учетных данных пользователя — имени и пароля — с помощью MSCHAPv2. После проверки NAC-система назначает пользователю соответствующую роль или политику доступа (например, VLAN или уровень сетевых прав). Таким образом, PEAP-MSCHAPv2 обеспечивает безопасную аутентификацию с использованием привычных паролей.

Сертификаты и структура X.509 v3

В PEAP-MSCHAPv2 сертификаты используются для подтверждения подлинности сервера и создания доверенного TLS-туннеля. Сертификат стандарта **X.509 v3** связывает открытый ключ с сервером и содержит идентификационные данные, сведения об издателе (CA), срок действия и цифровую подпись, подтверждающую подлинность. В версии X.509 v3 добавлены расширения, определяющие область применения ключа, альтернативные имена (например, DNS-имя сервера), политику доверия и механизмы проверки статуса.

Клиент проверяет сертификат сервера по цепочке доверия — от выданного серверу сертификата до корневого центра сертификации. Эта процедура гарантирует, что клиент подключается именно к доверенному серверу, а не к поддельной точке доступа. После успешной проверки создается TLS-туннель, через который передаются данные аутентификации.

Так как в PEAP-MSCHAPv2 сервер предъявляет сертификат, а клиент — нет, безопасность соединения полностью зависит от правильной проверки сертификата клиентом и корректной настройки цепочки доверия на стороне клиента.

Участие сертификата центра сертификации (CA)

Центр сертификации **(CA)** является ключевым элементом доверенной инфраструктуры PEAP-MSCHAPv2. Сервер аутентификации должен обладать сертификатом, подписанным доверенным CA, а клиент должен иметь корневой сертификат этого же CA в своем хранилище. При установлении соединения клиент сверяет подпись сертификата сервера с публичным ключом CA и проверяет срок действия и статус отзыва.

Если сертификат не выдан доверенным центром или его срок действия истек, соединение не устанавливается. Это защищает от атак типа *Man-in-the-Middle* и *Evil Twin*, при которых злоумышленник может создать поддельную точку доступа и перехватить данные пользователя.

Таким образом сертификат CA обеспечивает доверие между клиентом и сервером и служит основой для создания защищенного канала, внутри которого выполняется аутентификация MSCHAPv2. Вся безопасность PEAP-MSCHAPv2 зависит от корректности этой проверки и актуальности цепочки сертификации.

Безопасность и практическое применение

PEAP-MSCHAPv2 используется в AxelNAC благодаря поддержке со стороны Windows, macOS и большинства мобильных ОС. Он позволяет использовать существующие учетные записи домена без развертывания клиентских сертификатов.

Однако безопасность протокола ограничена стойкостью механизма **MSCHAPv2**, основанного на устаревших алгоритмах NTLMv1. При слабых паролях возможен их перебор при перехвате аутентификационного обмена. Поэтому рекомендуется использовать только сложные пароли, включать сетевое шифрование на уровне Wi-Fi (WPA2-Enterprise) и строго проверять подлинность сертификата сервера.

Настройка коммутатора в AxelNAC

Первым подготовительным этапом является первоначальная настройка коммутатора. Необходимо сконфигурировать коммутатор таким образом, чтобы он интегрировался с AxelNAC с помощью стандарта 802.1x.

Настройка стандарта 802.1x на коммутаторе

В рамках данного курса мы рассмотрим конфигурацию коммутатора на примере коммутатора доступа Cisco Catalyst 2960 с IP-адресом 172.21.2.3. Также, в примере зададим IP-адрес сервера AxelNAC 10.31.205.172.

Шаг 1. Подключитесь к этому коммутатору по протоколу SSH как администратор.

Шаг 2. Активируйте стандарт 802.1x на коммутаторе с помощью команды:

```
dot1x system-auth-control
```

Шаг 3. Настройте AAA таким образом, чтобы он использовал только что созданный сервер AxelNAC с помощью следующих команд:

```
aaa new-model
radius server AxelNAC
   address ipv4 10.31.205.172 auth-port 1812 acct-port 1813
   timeout 2
   key useStrongerSecret
aaa group server radius AxelNAC
   server name AxelNAC
aaa authentication dot1x default group AxelNAC
aaa authorization network default group AxelNAC
aaa accounting dot1x default start-stop group AxelNAC
radius-server vsa send authentication
aaa server radius dynamic-author
   client <IP> server-key <key>
   port 3799
snmp-server community useStrongerSecretSNMPRO RO
snmp-server community useStrongerSecretSNMPRW RW
```

Шаг 4. Настройте все (или только необходимые) порты для работы со стандартом 802.1x. В примере ниже выбран только порт №10:

```
interface fastEthernet 0/10
switchport mode access //определение порта как access-порт (нетегированного)
authentication host-mode multi-domain //режим аутентификации хоста multi-domain, разрешающий подключение нескольких конечных устройств на порт
authentication order dot1x mab //использование порядка методов аутентификации, при котором сначала выполняется попытка аутентификации по 802.1X, а затем — по MAB (MAC Authentication Bypass)
authentication priority dot1x mab //приоритеты методов аутентификации заданы так, чтобы 802.1X имел более высокий приоритет, чем MAB. Если оба метода проходят успешно, предпочтение отдается 802.
authentication port-control auto //аутентификация по 802.1x на порту
authentication periodic //периодическая реаутентификация клиента. Период по умолчанию составляет 3600 секунд
authentication timer restart 10800 //период реаутентификации (в секундах)
authentication timer reauthenticate 10800 //количество секунд до повторной попытки аутентифицировать неавторизованный порт
mab //включение MAC authentication bypass на порту, позволяя аутентифицироваться устройствам, не поддерживающим 802.1x
no snmp trap link-status //отключение отправки SNMP-ловушек при включении/отключении порта
dot1x pae authenticator //роль порта определена как аутентификатор. Он не будет отвечать на сообщения, предназначенные для суппликанта.
dot1x timeout quiet-period 2 //интервал ожидания (в секундах) после неудачной попытки аутентификации по 802.1x
dot1x timeout tx-period 3 //интервал ожидания ответа (в секундах) на EAP request перед его повторной отправкой
```

Шаг 5. Сохраните конфигурацию коммутатора.

Настройка коммутатора в AxelNAC

После того как выполнена конфигурация на стороне коммутатора, необходимо добавить его в AxelNAC, чтобы обучить их «общаться между собой». Для этого вы можете следовать алгоритму, описанному ниже:

Шаг 1. В AxelNAC перейдите в раздел **Конфигурация → Политики и контроль доступа → Сетевые устройства → Сетевые устройства** и нажмите **Новое сетевое устройство**. В выпадающем списке выберите значение **default**.

Шаг 2. На открывшейся странице заполните поля следующим образом:

- **IP-адрес/MAC-адрес/диапазон (CIDR):** 172.21.2.3;
- **Тип:** Cisco Catalyst 2960;
- **Режим:** Продуктивный.

Шаг 3. Переключитесь на вкладку **Роли** и убедитесь, что параметр **Назначать VLAN ID** (роль по идентификатору VLAN) активирован.

Шаг 4. Переключитесь на вкладку **RADIUS** и в поле **Секретная фраза** укажите секретную фразу, которую вы настроили на коммутаторе. В нашем примере секретная фраза — **useStrongerSecret**.

Шаг 5. На вкладке **SNMP** укажите необходимые значения в полях **Community Read** и **Community Write**. В поле **Версия** укажите **v2c**.

Заполните значения в соответствии с конфигурацией коммутатора:

- **Community Read** — useStrongerSecretSNMPRO;
- **Community Write** — useStrongerSecretSNMPRW.

Шаг 6. Для добавления коммутатора нажмите кнопку **Создать** в левом нижнем углу страницы.

Настройка центра сертификации (ЦС)

Вторым подготовительным этапом является установка и настройка центра сертификации (ЦС). В качестве ЦС может быть использовано различное ПО, поэтому данный этап должен быть изучен самостоятельно. После настройки ЦС, выпустите сертификаты для стороны сервера и стороны клиента.

Мы настоятельно рекомендуем выпускать сертификаты для клиентской стороны в виде контейнера с расширением **.pfx**, для упрощения следующих шагов.

После выпуска контейнера необходимо извлечь сертификаты для их установки. Данный процесс можно выполнить с помощью AxelNAC:

Шаг 1. Переместите ранее созданный контейнер сертификатов в AxelNAC, используя следующую команду, и введите пароль для доступа к AxelNAC:

scp <путь к контейнеру сертификатов> root@<IP-адрес AxelNAC}:~/{Контейнер сертификата}.pfx

Пример:
scp C:\Users\Default\downloads\Certificates.pfx root@{10.28.121.52}:~/Certificates.pfx

Шаг 2. Подключитесь к AxelNAC по SSH, создайте и переместите сертификат в удобную директорию с помощью следующего набора команд:

mkdir <папка для сертификатов>
mv /root/{Контейнер сертификата}.pfx <папка для сертификатов>/
cd <папка для сертификатов>

Пример:
mkdir certs
mv /root/Certificates.pfx certs/
cd certs

Шаг 3. В рабочей директории необходимо разделить сертификат на 3 части: Открытый ключ, сертификат УЦ, закрытый ключ. Во время разделения сертификатов у вас запросят пароль от контейнера:

openssl pkcs12 -in {Контейнер сертификата}.pfx -clcerts -nokeys -out <имя сертификата>.crt
openssl pkcs12 -in {Контейнер сертификата}.pfx -cacerts -nokeys -out <имя сертификата УЦ>.crt
openssl pkcs12 -in {Контейнер сертификата}.pfx -nocerts -out <имя закрытого ключа>.key

Пример:
openssl pkcs12 -in Certificates.pfx -clcerts -nokeys -out Axelnac_cert.crt
openssl pkcs12 -in Certificates.pfx -cacerts -nokeys -out Axeldemo_CA.crt
openssl pkcs12 -in Certificates.pfx -nocerts -out Axelnac_private_key.key

Шаг 4. Скорректируйте содержимое сертификатов: при экспорте через **openssl** могут появиться лишние данные, поэтому необходимо оставить только информацию о сертификатах (начиная с **------BEGIN CERTIFICATE------** и заканчивая **------END CERTIFICATE------**). Также необходимо инвертировать порядок указанных сертификатов так, чтобы первым был **сертификат УЦ** ближайший к клиенту.

Шаг 5. Полученные сертификаты необходимо перенести на АРМ, у которой есть доступ к веб-интерфейсу AxelNAC:

scp root@{IP-адрес AxelNAC}:~/<путь к файлу сертификата>/{Имя сертификата}.crt <Путь для переноса сертификата на АРМ>\{Имя сертификата}.crt
scp root@{IP-адрес AxelNAC}:~/<путь к файлу сертификата УЦ>/{Имя сертификата УЦ}.crt <Путь для переноса сертификата УЦ на АРМ>\{Имя сертификата УЦ}.crt
scp root@{IP-адрес AxelNAC}:~/<путь к файлу закрытого ключа>/{Имя закрытого ключа}.crt <Путь для переноса закрытого ключа на АРМ>\{Имя закрытого ключа}.crt

Пример:
scp root@{10.28.121.52}:~/scan_winrs_cert/Axelnac_cert.crt C:\Users\Default\downloads\Axelnac_cert.crt
scp root@{10.28.121.52}:~/scan_winrs_cert/Axeldemo_CA.crt C:\Users\Default\downloads\Axeldemo_CA.crt
scp root@{10.28.121.52}:~/scan_winrs_cert/Axelnac_private_key.key C:\Users\Default\downloads\Axelnac_private_key.key

Шаг 6. Для получения отпечатка сертификата на linux, воспользуйтесь командой:

openssl x509 -in {имя файла сертификата}.crt -fingerprint -sha1 -noout

Пример:
openssl x509 -in cert.crt -fingerprint -sha1 -noout

Установка сертификата на стороне клиента

Для того чтобы клиентское устройство могло быть подключено к серверу с аутентификацией по протоколу EAP-TLS, необходимо установить сертификаты на устройство. Поля, которые могут содержать сертификаты, показаны в таблице ниже.

Обязательные и опциональные поля сертификатов

Поле	Описание	Пример	Статус
UPN	User Principal Name пользователя	nb1@axeldemo.pro	Для выполнения аутентификации необходимо заполнить хотя бы одно из этих полей
CN	Common Name пользователя	nb1@axeldemo.pro	
DNS	DNS АРМ	nb1.axeldemo.pro	
IP Address	IP-адрес АРМ	192.31.205.15	Данные поля носят информационный характер и не требуют заполнения
Street Address	Географический адрес АРМ	ul. Lenina, 9A	
State or Province	Область/провинция/штат, для которого действителен сертификат	Mockovskaya oblast	
Country	Страна, для которой действителен сертификат	Honolulu	
Organizational Unit	Подразделение, для которого действителен сертификат	HR	
Organization	Организация, для которой действителен сертификат	AxelPRO	

Сертификат должен быть создан с включенной аутентификацией пользователя в EKU. В качестве имени пользователя в полях сертификата могут быть использованы атрибуты **UPN**, **CN** или **DNS**.

Шаг 1. Импортируйте сертификаты из контейнера сертификатов, следуя инструкциям мастера импорта сертификатов. При выборе хранилища сертификатов выберите **Личное**.

Шаг 2. Добавьте в автозагрузку сервис Windows **Проводная автонастройка** (dot3svc). Для этого откройте командную строку в Windows и введите следующий набор команд:

Set-Service -Name dot3svc -StartupType Automatic
Start-Service -Name dot3svc

Шаг 3. Откройте меню **Сетевые подключения**, затем откройте свойства сетевого интерфейса, по которому организовано подключение.

Шаг 4. На вкладке **Проверка подлинности** установите флажки для всех параметров.

Шаг 5. В поле **Метод проверки подлинности в сети** выберите значение **Microsoft: смарт-карта или иной сертификат**.

Шаг 6. Нажмите на кнопку **Параметры** справа от поля выбора метода и установите флажок для параметра **Подтверждать удостоверение сервера с помощью проверки сертификата**. Убедитесь, что дочерний параметр деактивирован.

Шаг 7. В поле **Доверенные корневые центры сертификации** выберите сертификат, ранее выданный ЦС.

Шаг 8. Перейдите в раздел **Дополнительно** и выберите корневого издателя сертификата. Затем нажмите **ОК** дважды.

Шаг 9. На вкладке **Проверка подлинности** нажмите **Дополнительные параметры**, и в поле **Указать режим проверки подлинности** установите **Проверка подлинности пользователя или компьютера**. Затем нажмите **ОК**.

Установка сертификата на стороне сервера аутентификации

Перед выполнением следующих шагов убедитесь, что при выпуске сертификата был установлен параметр "**аутентификация сервера**" для EKU (Extended Key Usage).

Для того чтобы сконфигурировать соединение с аутентификацией по протоколу EAP-TLS, необходимо установить сертификаты на сервере AxelNAC. Поля, которые могут содержать сертификаты, приведены в предыдущем параграфе.

Шаг 1. Перейдите на вкладку **RADUIS** в разделе **Конфигурация → Настройки системы → SSL-сертификаты** и нажмите **Редактировать**.

Шаг 2. На открывшейся странице замените предустановленные данные в полях **Сертификат сервера RADIUS**, **Закрытый ключ сервера RADIUS** и **Сертификат(ы) от центра сертификации** данными, полученными в ЦС и нажмите **Сохранить** в левом нижнем углу страницы.

После установки SSL-сертификата вам будет предложено перезапустить сервис **radiusd-auth**. Вы можете пропустить этот шаг, так как данный сервис в любом случае нужно будет перезапустить после окончательной настройки соединения.

Шаг 3. Перейдите в раздел **Конфигурация → Настройки системы → RADIUS → SSL-сертификаты PKI** и нажмите **Новый SSL-сертификат**.

Шаг 4. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Сертификат** — укажите сертификат, выпущенный ЦС для сервера;
- **Центр сертификации** — укажите сертификат удостоверяющего центра;
- **Закрытый ключ** — укажите закрытый ключ сертификата;
- **Пароль для закрытого ключа** — укажите пароль для контейнера сертификатов (при наличии);
- **Сертификат(ы) промежуточного центра сертификации (CA)** — при наличии промежуточного центра сертификации необходимо указать его сертификат, в ином случае, укажите сертификат удостоверяющего центра.

После этого нажмите **Создать** в левом нижнем углу страницы.

Шаг 5. Перейдите на вкладку **Профили TLS** и нажмите **Новый TLS-профиль**.

Шаг 6. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Профиль сертификата** — укажите имя SSL-профиля созданного в предыдущем шаге;
- **Минимальная версия TLS** — минимальная версия TLS, поддерживаемая подключаемыми устройствами;
- **Максимальная версия TLS** — максимальная версия TLS, поддерживаемая подключаемыми устройствами.

Мы рекомендуем выбирать минимальную версию TLS 1.2 и максимальную — 1.3, так как эти версии являются самыми актуальными.

После этого нажмите **Создать** в левом нижнем углу страницы.

Шаг 7. Перейдите на вкладку **Профили EAP** и нажмите **Новый профиль EAP**.

Шаг 8. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Тип EAP по умолчанию** — TLS;
- **Типы EAP-аутентификации** — TLS;
- **Профиль TLS** — укажите имя TLS-профиля созданного в предыдущем шаге.

После этого, нажмите **Создать** в левом нижнем углу страницы.

Шаг 9. Перезапустите службу **radiusd-auth**.

Настройка соединения с аутентификацией по протоколу EAP-TLS в AxelNAC

После того как сертификаты установлены на обеих сторонах, можно начинать настройку соединения в AxelNAC.

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Области** и нажмите **Новая область**.

Шаг 2. На вкладке **Основное** заполните поле **Область**, введя имя вашего домена.

Вы можете не создавать область, если создали ее ранее. В этом случае на вкладке **Области** нажмите на созданную вами ранее область, чтобы перейти в режим редактирования.

Шаг 3. На вкладке **Настройки EAP** выберите профиль EAP, который вы создали в шаге 8 установки сертификата на стороне сервера, и нажмите**Создать** в левом нижнем углу страницы.

Шаг 4. Перезапустите службу **radiusd-auth**.

Проверка работы соединения

После выполнения всех этапов конфигурации вы можете проверить работу соединения. Подключите клиентское устройство к порту коммутатора, на котором настроен dot1x. Клиентское устройство должно успешно авторизоваться и получить доступ в сеть.

Чтобы посмотреть, что происходит на стороне AxelNAC, перейдите в раздел **Аудит → Журналы аудита RADIUS** в интерфейсе администратора. Вы должны увидеть запись для MAC-адреса подключенного клиентского устройства. Щелкните строку с нужным MAC-адресом, чтобы увидеть логи обмена RADIUS-сообщениями. Если аутентификация 802.1X прошла успешно, в колонке **Статус узла** появится значение **Зарегистрировано**.

Также, вы можете подключиться к коммутатору по протоколу **ssh** и выполнить команду show authentication session interface <интерфейс, к которому подключено устройство> detail. В случае успешного подключения в строке **Status** будет указано значение **Authorized**.

ID статьи: 1442
Последнее обновление: 16 дек., 2025
Обновлено от: Ильина В.
Ревизия: 5
База знаний AxelNAC -> Обучающие материалы -> Обучающие курсы -> Конфигурация сетевых соединений -> Раздел 1. Аутентификация пользователей -> Глава 2. Аутентификация пользователей по протоколу PEAP-MSCHAPv2
https://docs.axel.pro/entry/1442/